UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR		ATTORNEY DOCKET NO.
09/120,763	07/22/98	ETZEL	M	ETZEL-5-3-11

TM02/1227

PETER H PRIEST
529 DOGWOOD DRIVE
CHAPEL HILL NC 27516

EXAMINER	
SEAL, J	
ART UNIT	**PAPER NUMBER**
2131	7

DATE MAILED: 12/27/00

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary

Application No.	Applicant(s)
09/120,763	Etzel Et. Al.
Examiner	**Group Art Unit**
James Seal	~~2766~~ 2131

☒ Responsive to communication(s) filed on 20 Oct 2000

☒ This action is **FINAL.**

☐ Since this application is in condition for allowance except for formal matters, **prosecution as to the merits is closed** in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11; 453 O.G. 213.

A shortened statutory period for response to this action is set to expire 3 month(s), or thirty days, whichever is longer, from the mailing date of this communication. Failure to respond within the period for response will cause the application to become abandoned. (35 U.S.C. § 133). Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

Disposition of Claim

☒ Claim(s) 1-18 is/are pending in the applicat

Of the above, claim(s) _____ is/are withdrawn from consideration

☐ Claim(s) _____ is/are allowed.

☒ Claim(s) 1-18 is/are rejected.

☐ Claim(s) _____ is/are objected to.

☐ Claims _____ are subject to restriction or election requirement.

Application Papers

☐ See the attached Notice of Draftsperson's Patent Drawing Review, PTO-948.

☐ The drawing(s) filed on _____ is/are objected to by the Examiner.

☐ The proposed drawing correction, filed on _____ is ☐ approved ☐ disapproved.

☐ The specification is objected to by the Examiner.

☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

☐ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

☐ All ☐ Some* ☒ None of the CERTIFIED copies of the priority documents have been

☐ received.

☐ received in Application No. (Series Code/Serial Number) _____.

☐ received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

*Certified copies not received: _____

☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

☐ Notice of References Cited, PTO-892

☐ Information Disclosure Statement(s), PTO-1449, Paper No(s). _____

☐ Interview Summary, PTO-413

☐ Notice of Draftsperson's Patent Drawing Review, PTO-948

☐ Notice of Informal Patent Application, PTO-152

— SEE OFFICE ACTION ON THE FOLLOWING PAGES —

DETAILED ACTION

1. This action is a response to you correspondence of 20 April 2000

2. No new amendment filed.

3. Previous Office actions are incorporated herein.

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

5. Claims 1-18 are pending.

Claim Rejections - 35 USC § 103

6. Rejection to claims 1-18 are maintained.

Response to Amendment

7. Applicant's arguments filed 20 October 2000 have been fully considered but they are not persuasive.

8. Alanara discloses the CMEA algorithm as the applicant agrees on page 2, line 5. It is well know in the art that any algorithm which performs encryption, may be iterated multiple times to increase the security of the encryptions. This concept date back to Claude Shannon, Communication Theory of Secrecy Systems 1945, section 3, reprinted in Shannon's Collected Papers, Edited by Sloane and Wyner, IEEE Press or in the work of Feistel on Lucifer and DES, see Schneier Applied Cryptography (October 1995) chapter 12. Thus iteration is a well established principle in the art of cryptology. Performing transformations (such as permutations

of bits, bit rotations, bit swapping, etc.) on data streams before and after say is also a well established technique in the cryptology and was also advocated by Feistel as a means of confusion (as opposed to diffusion). The employment of tboxes together with CMEA's has also been used for cellular as discussed in Appendix A to IS-54 (Feb 1992). The use of Table Lookup to speed up calculations has not only been used in the cryptographic arts (see previous document, Schneier, and in particular the work of Feistel on Lucifer and DES), but is standard practice in computer science. The combination of such techniques is strongly suggested by Feistel in his work on Lucifer and DES and as applied over the years to nearly all of the AES cryptosystems. That one in the cryptographic arts would not be motivated to apply these arts to the teachings of Alamara and his implementation of CMEA (Cellular Message Encryption Algorithm) would be very surprising considering the teaching of Shannon and the application his work by Fiestel to any encryption scheme. The motivation to combine is to be taken broadly over the art and the motivation to combine does not need to be found in the four corners of the prior art.

9. The teachings of Vernan and Friedmann, classical cryptographers, was used to note that the specific form of the applicant's algorithm is not new and that it is applied to many cryptosystem where simplicity and security is needed. The Vernan (one-time-pad) is well known for its security and the specific formulas of the applicant are a mathematical representation of his double tape encryption scheme, further modified by Friedman.

10. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date.

Conclusion

11. Any inquiry concerning this communication should be direct to James Seal at telephone number (703) 308 4562. The examiner can normally be reached on Monday through Friday from 7:30 a.m. to 5:30 p.m.

12. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail Hayes, can be reached at (703) 305-9711.

13. Any inquiry of a general nature or relating to the status of this application or preceding should be directed to the Group receptionist, whose telephone number is (703) 305-3800. Fax number is (703) 305 0040.

James Seal

James Seal

21 December 2000

Gail Hayes

GAIL HAYES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100